REMARKS

The present Amendment is submitted with a Request for Continued Examination that is provided herewith. Authorization is provided herewith to pay any underpayment of fees or credit any overpayment of fees to Deposit Account No. 02-4800.

I. AMENDMENT OF THE CLAIMS

The claims have been amended as may be appreciated from the listing of claims provided herewith. Claims 7-20 and 26-31 are pending. The currently pending claims include independent claims 7, 26 and 30. The dependent claims depend directly or indirectly from claims 7, 26 or 30.

II. RESPONSE TO THE REJECTION OF THE CLAIMS

The Examiner rejected all the previously presented pending claims under 35 U.S.C. § 103 in view of the combination of U.S. Patent Application Publication No. 2003/0167343 to Furuno and U.S. Patent Application Publication No. 2006/0107060 to Lewis et al. in the Final Office Action dated February 17, 2009 (hereafter "Final Office Action").

A. Burden Of Proving Obviousness Under 35 U.S.C. § 103

"**All words in a claim must be considered in judging the patentability of that claim against the prior art**." MPEP § 2143.03 (emphasis added). "When evaluating claims for obviousness under 35 U.S.C. 103, **all the limitations of the claims must be considered and given weight**." MPEP § 2143.03. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *Id.* "A 35 U.S.C. 103 rejection is based on 35 U.S.C. 102(a), 102(b), 102(e), etc. depending on the type of prior art reference used and its publication or issue date." MPEP § 2141.01.

To establish a *prima facie* case of obviousness, an Examiner must show that an invention would have been obvious to a person of ordinary skill in the art at the time of the invention. MPEP § 2141. "Obviousness is a question of law based on underlying factual inquiries." *Id.* The factual inquiries enunciated by the Court include "ascertaining the differences between the claimed invention and the prior art" and "resolving the level of ordinary skill in the pertinent art." MPEP § 2141.

"A statement that modifications of the prior art to meet the claimed invention would have been 'well within the ordinary skill of the art at the time the claimed invention was made' because the references relied upon teach that all aspects of the claimed invention were individually known in the art is not sufficient to establish a *prima facie* case of obviousness without some objective reason to combine the teachings of the references." MPEP § 2143.01. "[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead**, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.**" MPEP § 2143.01 (citing *KSR*, 550 U.S. at ___, 82 USPQ2d at 1396) (emphasis added).

Moreover, "[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious." MPEP § 2143.01. Also, "the proposed modification cannot render the prior art unsatisfactory for its intended purpose." MPEP § 2143.01.

B. The Cited Combination Fails To Teach Limitations Of Pending Claims 7-20 And 28-29

The Examiner cites Lewis et al. as disclosing storing status information for a communication terminal in a memory associated with the communication terminal, providing the status information with a digital signature calculated from the status information by a private key for an asymmetrical encoding method, transmitting the status information as the digital signature to a gatekeeper and checking the digital signature for the event of a positive check result. (Final Office Action, at 3). The Examiner admits that Furuno does not disclose such features. (Final Office Action, at 2-3).

Lewis et al. disclose a method for authenticating a cellular telephone based on a "smart chip." The smart chip has its own unique private key and public key that are used to authenticate the chip and a device to which the chip is attached to a server. (¶¶ 73-78). A central server verifies the identity of the smart chip of a digital device by extracting the public key of the smart chip from a descriptor sent to the server and transmits random data using the public key and the predefined public/private key identity encryption algorithm and transmits that data to the digital device requesting the smart chip to decrypt that message. (¶ 74). Upon receipt of the encrypted message from the server, the smart chip decrypts the data by accessing its private key. The decrypted data is then transmitted to the central server. (¶ 75). The central server receives the decrypted data and compares the returned data with the original randomly generated data. If the data matches, then the public key in the descriptor data belongs to the physical smart chip making the request, which verifies the smart ship's identity. (¶ 76).

As may be appreciated from the listing of claims, Lewis et al. do not teach numerous limitations of the currently pending claims 7-20 and 28-29.

1. The Cited References Do Not Disclose:

providing status information to a communication terminal, the status information comprising a digital signature calculated from status information of the communication terminal by a private key of the first control unit, the first control unit being associated with the communication terminal for the resolution and/or conversion of network addresses

The private/public key authentication system disclosed by Lewis et al. do not teach or suggest a control unit such as, for example, a gateway, that provides status information that includes a digital signature calculated from the status information by a private key of the first control unit. To the contrary, Lewis et al. teach that a digital device, such as a cell phone, must have a private key, which is not known to other devices, and that the control unit must also have a separate, unique private key. (¶¶ 17, 22, 73-78). Moreover, the control unit disclosed by Lewis et al. does not provide a digital signature to the digital device that is based on the private key of that control unit. (¶¶ 73-78).

Further, as the Examiner admits, Furuno does not disclose any control unit providing status information with a digital signature. (Final Office Action at 3). Therefore, even the impermissible combination of both Furuno and Lewis et al. fail to teach or suggest this limitation.

a. Lewis et al. Cannot Be Modified To Render The Claims Non-Obvious

Changing the invention disclosed by Lewis et al. to require a control unit to provide a digital signature to a communication terminal based on that control unit's private key would impermissibly change the principle of operation of the authentication system disclosed by Lewis et al. MPEP § 2143.01. The "smart chip" disclosed by Lewis et al. is configured to ensure that a

unique private key for each "smart chip" exists. (Abstract; ¶¶ 17 & 22). The private key of the "smart chip" cannot be read outside that chip. (Abstract; ¶¶ 17 & 22).

The digital signature of the status information provided by the first control unit is based on the first control unit's private key. A private key for the communication terminal that is only known to that communication terminal is not required by the pending claims. The lack of such a private key known only to the communication terminal would require the principle of operation of the authentication system disclosed by Lewis et al. to be drastically altered. For instance, the "smart chip" would have no function in such a system. Moreover, such an alteration of Lewis et al.'s "smart chip" would render the system disclosed by Lewis et al. inoperable.

b. Lewis et al. Teach Away From The Pending Claims

Lewis et al. specifically teach that a digital device, such as a cell phone, should have its own "smart chip" with its own separate, unique private key. (¶ 22). This teaches away form the claimed invention, which requires a first control unit to provide a digital signature to a communication terminal that is calculated based on the first control unit's private key.

2. The Cited Art Does Not Disclose:

checking the digital signature with the at least one second control unit, the at least one second unit configured to access the public key of the first control unit to check the digital signature

The private/public key authentication system disclosed by Lewis et al. does not suggest checking a digital signature by using a public key of a different control unit to help check the digital signature of a communication terminal. Indeed, Lewis et al. do not teach or suggest use of any second control unit for checking a digital signature. Lewis et al. only teach the use of a smart chip and a first server for checking digital signatures. There is no teaching of having a

second control unit use a public key of a first control unit to check a digital signature of a communication terminal.

Moreover, as the Examiner admits, Furuno does not disclose any control unit checking a digital signature. Therefore, even the impermissible combination of both Furuno and Lewis et al. fail to teach or suggest this limitation.

3. The Cited Art Does Not Disclose:

Depositing a public key of a first control unit such that at least one second control unit is able to access that public key

The private/public key authentication system disclosed by Lewis et al. does not utilize or suggest depositing a public key of a first control unit so one or more second control units can access that public key. Indeed, Lewis et al. do not teach or suggest use of any second control unit for accessing a public key of a first control unit. Moreover, Furuno does not disclose any second control unit that can access the public key of a first control unit. Therefore, even the impermissible combination of both Furuno and Lewis et al. fail to teach or suggest this limitation.

C. The Cited References Do Not Teach The Limitations Of Claims 26-27

Claim 26 requires a communication terminal to store at least one portion of status information in a memory unit that is comprised of a digital signature calculated from the status information by a first control unit associated with the communication terminal and is asymmetrically encoded using the private key of the first control unit. Claim 27 depends from claim 26 and, therefore, also contains this limitation.

As discussed above with respect to claims 7-20, neither Lewis et al. nor Furuno disclose any storage of status information that has such a digital signature. Indeed, Lewis et al. teach

away from such a digital signature in paragraph 22. Moreover, as discussed above with respect to claims 7-20 and 28-29, Lewis et al. cannot be combined with Furuno. For at least these reasons, claims 26-27 are allowable over the cited art.

Claims 26 and 27 also require a communication terminal to be configured to determine if a first control unit has failed to properly update the at least one portion of status information and, if the first control unit fails, send a request to be transmitted to at least one second unit to associate the communication terminal with the at least one second unit. There is no suggestion or disclosure of a communication terminal configured to determine that a control unit has failed to update the status information of the communication terminal in either Lewis et al. or Furuno.

Moreover, there is no teaching or suggestion in either Lewis et al. or Furuno of the communication terminal associating with a second control unit as a result of a first control unit failing to update the status information of the communication terminal. Furuno discloses that end points attempt to register with a second gatekeeper when the primary gate keeper rejects their registration attempt upon startup of the endpoints. (¶¶ 8-10). Lewis et al. is silent with respect to a second control unit or any failure of a first control unit.

For at least the above reasons, claims 26 and 27 are allowable over the cited art.

D. Claims 30-31 Are Allowable Over The Cited Art

As discussed above, Lewis et al. and Furuno cannot be properly combined. For at least this reason, claims 30-31 are allowable over the cited art. Moreover, the combination of Furuno and Lewis et al. fail to disclose each and every limitation of claims 30-31.

For example, both claims 30 and 31 require providing status information for a communication terminal that includes a digital signature calculated from status information of

the communication terminal by a private key of the first control unit such that the digital signature is asymmetrically encoded. There is no teaching or suggestion of such a digital signature in Furuno or Lewis et al. Indeed, Lewis et al. teach away from this limitation. Lewis et al. teach that a digital signature of a communication terminal should be defined in a smart chip that can only be read by the smart chip. (¶ 22). Lewis et al. do not teach or suggest a digital signature calculated from status information by a private key of a first control unit such that the digital signature is asymmetrically encoded.

III. CONCLUSION

For at least the above reasons, reconsideration and allowance of all pending claims are respectfully requested.

Respectfully submitted,

/Ralph G. Fischer/

Dated: April 9, 2009

Ralph G. Fischer
Registration No. 55,179
BUCHANAN INGERSOLL & ROONEY PC
One Oxford Centre
301 Grant Street
Pittsburgh, Pennsylvania 15219

(412) 392-2121

Attorney for Applicant